



MASTER

DEPARTMENT OF THE NAVY

COMMANDER MOBILE MINE ASSEMBLY GROUP

2536 FOURTH STREET

N. CHARLESTON, S.C. 29406-6171

IN REPLY REFER TO:

COMOMAG/MOMAGINST 5230.1C

Code N01F

01 November 1994

COMOMAG/MOMAGINST 5230.1C

Subj: UTILIZATION OF AUTOMATED INFORMATION SYSTEMS (AIS)

Ref: (a) SECNAVINST 5239.2  
(b) OPNAVINST 5239.1A  
(c) CINCLANTFLTINST 5239.1  
(d) COMINWARCOMINST 5239.1C  
(e) DOD 5200.28-STD "Orange Book" (NOTAL)  
(f) DODINST 5215.2  
(g) COMOMAG/MOMAGINST 5040.1F  
(h) OPNAVNOTE C5510 SER 09N  
(i) COMOMAG/MOMAGINST 4000.1L  
(j) DOD Magnetic Remanence Security Guidelines (CSC-STD-005-85)

COMOMAG  
ORIGINAL

Encl: (1) Definition of Terms  
(2) Sample Abbreviated System Decision Paper (ASDP)  
(3) Sample Appointment Letters  
(4) ADP Security Training Sources  
(5) Sample Accreditation Letter  
(6) COMOMAG AIS Contingency Plan  
(7) Access Warning Message  
(8) PC Maintenance Requirement Card (MRC)  
(9) Printer Maintenance Requirement Card (MRC)  
(10) Sample Diskette Directory Listing  
(11) Sample Diskette/Tape Inventory Notification Memorandum  
(12) Personal Computer Operator PQS

1. Purpose. To provide guidance concerning utilization and security of Automated Information Systems (AIS) at COMOMAG and subordinate sites. Enclosure (1) contains definitions for terms used in this instruction.

2. Cancellation. COMOMAG/MOMAGINST 5230.1B

3. Objective. To ensure all Automated Information Systems (AIS) utilized by COMOMAG staff and subordinate MOMAG sites are afforded proper operational and security considerations required to adequately protect equipment, data processed and personnel who operate related equipment from undue harm or loss. This objective will be met by ensuring proper software and physical, administrative and operational security countermeasures are established and personnel responsible for using AIS equipment are provided proper training in its use.

MASTER

1 NOV 1994

4. Policy. All MOMAG AIS equipment will be operated in accordance with AIS security requirements outlined in references (a) through (d) and will be utilized for official business only. No privately owned or leased AIS equipment or software will be installed or utilized at COMOMAG Headquarters or the MOMAG sites without specific written permission from COMOMAG and such permission will be limited to instances of critical need only. To protect against introduction of computer viruses to MOMAG systems, strict virus screening procedures will be established and adhered to and importation of data from unofficial sources is strictly prohibited. Software copyright laws must be strictly observed. All community software will be copied and distributed in strict accordance with copyright requirements and no unauthorized software will be installed on MOMAG systems. The Controlled Access Protection (CAP) C2 functionality defined in reference (e) shall be implemented on all community networks and computer systems which process classified or sensitive unclassified data. To ensure uniformity in MOMAG AIS hardware and software, and to ensure the most cost effective procurement sources are utilized, all MOMAG AIS funding requests submitted to competent authority and all hardware/software procurement actions not accomplished by COMINELWARCOM will be accomplished by COMOMAG. AIS requirements identified by MOMAG sites will be submitted to COMOMAG for consolidation into a single AIS requirement.

5. Scope. This instruction applies to all AIS equipment and computer networks installed at COMOMAG and its subordinate activities and provides guidance concerning AIS equipment operation, security and training.

6. Responsibilities

a. COMOMAG. Responsible for:

(1) Serving as Designated Approval Authority (DAA) for COMOMAG Headquarters AIS equipment.

(2) Ensuring AIS equipment installed at COMOMAG Headquarters is:

(a) Operated in accordance with this instruction.

(b) Accredited in accordance with the policy and procedures outlined herein and as prescribed by references (a) through (d).

(3) Ensuring an Automated Data Processing Security Officer (ADPSO) and a Network Security Officer (NSO) and/or Terminal Security Officer (TSO) are appointed for COMOMAG staff.

(4) Ensuring all instances of infection by computer viruses are promptly reported to the Navy Computer Incident

1 NOV 1994

Response Team (NAVCIRT) in accordance with references (e) and (f) as expanded by NAVELEXSECCEN 240243Z AUG 93.

(5) Ensuring a contingency plan for the staff computer network and AIS equipment is in place.

(6) Developing and submitting funding requests for AIS assets to competent authority.

(7) Developing required Life Cycle Management documentation in support of AIS funding requests.

(8) Procuring AIS assets funded by competent authority.

(9) Establishing utilization policy for MOMAG AIS equipment.

(10) Providing guidance concerning the security, training, operation and maintenance of AIS assets.

(11) Ensuring compliance with this instruction and references (a) through (e) via administrative inspections as outlined in reference (g).

b. Commanding Officers and Officers in Charge.  
Responsible for:

(1) Serving as Designated Approval Authority (DAA) for AIS equipment installed at their activity.

(2) Ensuring AIS equipment installed at their activity is:

(a) Operated in accordance with this instruction.

(b) Accredited in accordance with the policy and procedures outlined in this instruction and references (a) through (d).

(3) Ensuring an Automated Data Processing Security Officer (ADPSO) and, when applicable, a Network Security Officer (NSO) and/or Terminal Security Officer (TSO) are appointed for their activity.

(4) Ensuring all instances of infection by computer viruses are promptly reported to the Navy Computer Incident Response Team (NAVCIRT) in accordance with references (e) and (f) as expanded by NAVELEXSECCEN 240243Z AUG 93. COMOMAG will be an info addressee on all related correspondence.

(5) Ensuring all AIS security infractions which jeopardize mission critical systems are promptly reported to COMOMAG.

1 NOV 1994

(6) Ensuring a contingency plan for all mission critical AIS systems is in place.

(7) Documenting additional AIS requirements in accordance with enclosure (2) and submitting such requirements to COMOMAG.

(8) Identifying local sources for computer hardware maintenance support if available, and for submitting funding requirements to COMOMAG.

(9) Negotiating written off-site support agreements with activities in their locality.

c. ADP Security Officer (ADPSO). Each CO/OIC will officially appoint an ADPSO for their command. The appointment will be in writing and shall conform to the format outlined in enclosure (3). The ADPSO will perform the responsibilities outlined below, as well as those added requirements a CO/OIC might deem necessary. All personnel who are appointed to serve as ADPSO must complete certified ADP Security Officer training. Enclosure (4) contains a partial list of activities who provide ADP security training. COs/OICs should conduct a survey of local government activities to determine if comparable training is available in their locality before they submit funding requests for AIS security training. ADPSO's are responsible for:

(1) Developing, implementing and maintaining command AIS security programs.

(2) Developing, implementing and maintaining a command AIS user training and Personal Qualification Standard (PQS) program.

(3) Providing AIS security briefs to all incoming personnel within 30 days of reporting and for providing annual AIS security training for all hands.

(4) Developing, testing, implementing and maintaining command AIS contingency plans.

(5) Developing and implementing a comprehensive command anti-virus familiarization and screening program.

(6) Completing all reference (a) through (d) AIS accreditation requirements for command systems.

(7) Maintaining a current inventory of command AIS hardware and software.

(8) Reporting AIS security violations to the CO/OIC.



1 NOV 1994

(9) Documenting and reporting incidents of virus infections to the CO/OIC.

(10) Documenting additional AIS requirements in accordance with enclosure (2).

d. Network Security Officers (NSO). Each CO/OIC whose command has a computer network installed shall appoint an NSO for their command. The appointment will be in writing and shall conform to the format outlined in enclosure (3). The NSO will perform those NSO responsibilities outlined below as well as those added requirements a CO/OIC might deem necessary. A single appointee may serve as both ADPSO and NSO. The ADP Security training specified for ADPSOs must also be provided for those Personnel who are appointed to serve as NSO. NSO's are responsible for:

(1) Administering command computer networks.

(2) Assisting the ADPSO in administering the Command AIS Security program as it pertains to command computer networks.

(3) Developing, implementing and maintaining a network user training and Personal Qualification Standard (PQS) program for the command.

(4) Assisting the ADPSO in completing all AIS accreditation requirements for command computer networks.

(5) Reporting all network security violations to the ADPSO.

e. Terminal Security Officers (TSO). Each CO/OIC whose command routinely conducts remote terminal sessions on systems located at other government activities shall appoint a TSO for their command. The appointment shall be in writing and shall conform to the format outlined in enclosure (3). The host activity will be provided an original copy of the appointment letter. The TSO will perform those TSO responsibilities outlined below as well as those added requirements specified by the host activity. TSO's are responsible for:

(1) Preparing and forwarding user access requests to host activities.

(2) Issuing user passwords forwarded by the host activity and submitting required reports.

(3) Informing the ADPSO and terminal users of host activity security requirements.

(4) Ensuring security measures specified by the host activity are adhered to during remote terminal sessions.

1 NOV 1994

(5) Reporting all breaches of terminal security to the host activity and the ADPSO.

7. Security. References (a) through (d) specify the policies, procedures and responsibilities for establishing and maintaining AIS security programs within the Navy and will be adhered to by COMOMAG and its subordinate commands.

a. Training. All personnel who utilize AIS equipment will receive an AIS security brief from the ADPSO within 30 days of reporting to a MOMAG activity. In addition, all users will receive annual AIS security training.

b. Accreditation. Accreditation is a formal authorization statement by a Designated Approval Authority (DAA) to operate an AIS or computer network in an environment which provides processing security commensurate with a set of security requirements derived from an approved risk management process. Each computer system and computer network installed at a MOMAG facility will be assigned a system ID which includes the department abbreviation plus a sequential number (i.e., OPS-01). Each system will be accredited in accordance with procedures outlined in reference (b). Systems which have identical configurations and processing requirements may be grouped for accreditation. A copy of the accreditation letter shall be forwarded to COMOMAG and shall conform to the format outlined in enclosure (5). All AIS and computer networks which process sensitive unclassified or classified data must meet C2 trust level requirements to be accredited. At a minimum, the following risk management process will be completed before accreditation is granted:

(1) Security Survey. The Security Survey contained in chapter (5) of enclosure (2) to reference (b) will be completed for each AIS and computer network. An automated version of this form may be utilized where available.

(2) Activity AIS Security Plan. An Activity AIS Security Plan (AAISSP) will be developed for the activity in accordance with chapter (7) of enclosure (2) to reference (b).

(3) TEMPEST. Reference (f) excludes all MOMAG activities from TEMPEST review requirements. However, COMOMAG and the MOMAG sites will observe proper TEMPEST profiles in accordance with paragraph 7c of this instruction.

(4) Contingency Plan. COMOMAG and the MOMAG sites will develop a command AIS Contingency Plan which defines emergency backup processing and recovery procedures for each AIS or computer network on which mission critical applications are processed. Mission critical applications are applications which could unduly hinder or prevent an activity from meeting its mission objectives if they were not available and include such routines as MTF Editor, MDU, MDS, GATEGUARD, SCAAIR, DAMES and

1 NOV 1994

similar systems. Systems on which no mission critical applications are performed shall be identified in the plan as having no contingency requirement. Each Contingency Plan will follow the sample outlined in enclosure (6) and will:

(a) Identify those persons responsible for carrying out each action.

(b) Identify the systems and equipment involved.

(c) Identify the software, supplies and documentation required.

(d) Identify an off-site backup processing and storage facility where backup processing support can be obtained and copies of all required software, supplies and documentation can be stored. COs/OICs will negotiate off-site support agreements with other activities in their locality.

(e) Outline preparations required prior to a disruption of services.

(f) Specify the emergency backup and recovery procedures to be followed in the event of temporary disruptions, partial loss of assets and/or facility and total loss of assets and/or facility.

(5) Accreditation Report. An accreditation report will be drafted and stored with other support documentation.

(6) Accreditation Support Package. An accreditation support package containing copies of all documentation generated in the risk management process will be assembled and retained by the ADPSO.

c. TEMPEST Requirements. Reference (h) exempts COMOMAG and the MOMAG sites from TEMPEST review requirements. However, all MOMAG activities will continue to observe proper TEMPEST profiles for those AISs on which classified data is processed. To ensure the most suitable TEMPEST environment is maintained, each CO/OIC will utilize the following guidelines for selecting and placing AIS equipment on-site:

(1) Systems with removable hard drives will be utilized for classified processing unless specifically authorized by COMOMAG. The security and disposal measures outlined in paragraph 7(o) of this instruction will be implemented for all hard drives, removable or fixed, which contain classified data.

(2) Locate the system in an area in which a 16 to 20 meter distance from the system could reasonably be considered controlled (i.e., under constant surveillance).

1 NOV 1994

(3) Do not locate the system in front of an unshielded window.

(4) Ensure that RFI filters provided for a system are properly installed and utilized.

(5) Whenever possible, locate the system a minimum of 3 meters from the nearest telephone. Although no longer a requirement, this is a good security practice.

(6) Do not allow transmitters to be located in the space. These devices can transmit data signals beyond the controlled space.

d. User Access. COMOMAG and its subordinate commands shall follow the "**least privileged**" principle as defined in reference (e) under which a user will be granted access to an AIS and its information only when they have a certified "**need to know**" and posses the required security clearance. If either of these criteria is absent, user access shall default to "**no access.**" This rule applies to all information including classified, "Official Use Only" and Privacy Act data.

e. Access Warnings. Each AIS and computer network will display the access and monitor warning messages listed in enclosure (7) each time the system is booted and/or network LOGON procedures are initiated.

f. Passwords. Access to MOMAG computer systems and networks shall be controlled by user ID's and user passwords. NSO's will assign network user ID's, establish a network user account and assign an initial user password for each authorized user. User passwords shall be 8 characters in length and shall be changed every 90 days. Birth dates, social security numbers, phone numbers, names of relatives or pets, job related acronyms and other easily decipherable items shall not be utilized as passwords. The use of upper and lower case characters as well as a mixture of alpha and numeric characters is encouraged. All users shall afford their passwords the safeguards required for the highest data classification to which they have access. They will not divulge their password to other users nor allow other personnel to utilize their password to access an AIS or computer network.

g. Communications Security. All classified data transmissions within the MOMAG community shall be accomplished via an National Security Agency (NSA) approved encryption device (i.e. STU III) only. Under no circumstances will MOMAG activities utilize commercial or shareware encryption routines or any other mechanism to attempt transmission of classified information via uncertified data modems.

1 NOV 1994

h. Network Security. All MOMAG activities which utilize computer networks shall have an NSO appointed for each network installed and all networks shall meet CAP C2 standards. All network users will receive network operation and security training before a network user account and password are issued. Users who are granted access will comply with all network operational and security requirements and will:

(1) Protect network passwords at all times.

(2) Not allow other members to utilize their password to access the network.

(3) Not leave workstations unattended while connected to the network.

(4) Disconnect workstations at the completion of each session.

(5) Not allow other members to view sensitive unclassified or classified data when they do not have a "need to know" and the required security clearance.

(6) Notify the NSO when access to the network is no longer required.

i. Remote Terminal Security. Each AIS utilized to routinely access remote computer systems (i.e. CAIMS, IDAFMS, etc.) shall have a TSO assigned for each system accessed. Users who are granted access to remote systems via dial-up or NAVNET communication links shall receive terminal security briefing prior to granting them access. Terminal users will comply with all operational procedure specified by the TSO and the host activity. In addition, they will:

(1) Protect their user password at all times.

(2) Not allow other members to utilize their password to access the remote system.

(3) Not leave a terminal unattended while it is connected to the remote system.

(4) Disconnect the terminal at the completion of each terminal session.

(5) Not allow other members to view sensitive unclassified or classified data when they do not have a "need to know" and the required security clearance.

(6) Notify the TSO when access to the remote system is no longer required.



1 NOV 1994

j. Physical Security. Normal office work spaces usually provide adequate environmental controls to ensure proper AIS operation. The added protection required to safeguard AIS equipment against unauthorized access, theft and malicious acts will be determined by the security posture of the spaces in which it is located. For example, an AIS located in a building which is itself located in a restricted, fenced area or which is routinely locked outside normal working hours may require no additional physical security. However, if that same equipment is located in a building with open access, it must be placed in a secure space outside normal working hours and access to the equipment must be monitored during working hours. Wherever possible, access to AIS spaces will be restricted to authorized personnel only. If access cannot be restricted, visitors will be escorted at all times. In regard to data security, a combination of physical access (escorts) and procedural controls (SOPs) will be employed to protect data from unauthorized disclosure, modification or destruction. Information sensitivity and equipment susceptibility to theft should be major considerations when determining the physical security measures which must be implemented for data and/or AIS equipment.

k. Hardware Security. As used in this instruction, the term hardware refers to those physical components which make up an AIS. These include CRTs, keyboards, system units, printers and other peripheral devices. The following requirements are hardware specific:

(1) All AIS equipment including such items as printer ribbons (when installed) must display a label which identifies the highest classification of data that may be processed on that equipment.

(2) The ADPSO will maintain a current inventory of all AIS equipment assigned to the activity and will conduct an annual inventory of that equipment. The inventory requirements specified for controlled equipage/minor property items in reference (i) satisfy this requirement.

(3) AIS hardware will be stored in a secure space whenever the facility is unmanned.

(4) AIS equipment will be operated within the temperature ranges specified by the manufacturer.

(5) Adequate lighting will be provided in AIS spaces including emergency lighting where natural lighting is not available.

(6) Where possible, AIS equipment will be provided a dedicated power outlet. Facilities which experience frequent power fluctuations or AISs on which data sensitive applications (i.e. financial applications, network servers, etc.) are processed shall be equipped with battery backup systems and/or



1 NOV 1994

line voltage regulators. All network servers shall be equipped with a battery backup system.

(7) Whenever possible, AIS equipment will not be installed in spaces which have overhead plumbing or sprinkler systems. When this situation cannot be avoided, a plastic covering must be readily available within the space to protect the equipment from water damage.

(8) AIS equipment will not be located in the vicinity of a strong magnetic field or in spaces exposed to direct radiation from sources such as radar equipment, etc.

(9) AIS equipment will not be located near a coffee mess, scuttlebutt or any other area where groups tend to gather.

(10) Smoking, eating and drinking will not be allowed in the immediate vicinity of an AIS.

(11) Operators will not be allowed to pound or otherwise abuse the keyboard, printer, CRT or system unit.

(12) AIS equipment will not be placed on flimsy tables such as typewriter tables.

(13) Personnel who have not received maintenance training will not be allowed to replace components in the unit and under no circumstances will any personnel be allowed to attempt repairs or component replacements beyond those defined in the "Owner's Manual" unless otherwise authorized by COMOMAG.

(14) Adequate fire protection will be available for AIS spaces. Carbon dioxide or other authorized electrical fire extinguishers will be utilized. Halon extinguishers may be utilized until they are phased out in FY95.

(15) A routine Preventative Maintenance System (PMS) schedule will be established for AIS equipment. Personnel assigned PMS duties will utilize enclosures (8) and (9) for AIS maintenance.

1. Software Security. As used in this instruction, the term software refers to any Navy, commercial, shareware or locally developed programs which can be executed on a micro computer and the documentation which accompanies it. These include such items as word processors, spreadsheets, utilities and other routines. The following requirements are software specific:

(1) The ADPSO will maintain a current inventory of all software assigned to the activity and will conduct an annual inventory of that software. The inventory requirements specified

1 NOV 1994

for controlled equipage/minor property items in reference (i) satisfy this requirement.

(2) A backup copy will be made of each software application. These copies will be utilized for program installation tasks. The copies and the original disks will be stored in secure spaces apart from each other.

(3) The copyright laws specified for each software package will be observed. No software will be copied or distributed except in strict accordance with copyright specifications.

m. Diskette Security. Data diskettes are sensitive storage devices which are widely used for storing and/or transporting small amounts of data. The following safeguards will be afforded all data diskettes:

(1) All diskettes on which information of continuing importance is stored will be controlled in accordance with the procedures outlined in the diskette management section of this instruction and shall display a label which reflects the highest classification of data stored on the disk.

(2) A felt tip pen will be used when writing information on a label that is affixed to a diskette.

(3) Diskettes will be stored in a controlled environment such that they are not subjected to extreme fluctuations in temperature. No diskette will be placed and/or stored in direct sunlight.

(4) Diskettes will not be placed on or near a magnetic source such as a paper clip holder, radio or electronic recording device while in operation. Magnetic fields generated by these sources can corrupt data on a diskette.

(5) Diskettes will not be folded, bent or mutilated.

(6) Staples and paper clips will not be used to secure diskettes to documents, folders, etc. Rubber bands will not be used to bind 5 1/4 inch diskettes together.

(7) There will be no attempts to clean surfaces of diskettes.

(8) Diskettes will not be used as a Frisbee, as coasters for coffee or soft drinks, or otherwise subjected to abuse.

n. Data Security. Safeguarding official information processed on AIS equipment must be afforded the highest priority since the loss or compromise of such data can seriously hinder a command's ability to meet mission objectives. In addition, the

1 NOV 1994

investment required to compile and/or recover such data represents a major cost in terms of money and manpower. Accordingly, all MOMAG activities will ensure the data security requirements outlined below are strictly observed.

(1) Each AIS must display a label identifying the highest classification of data which may be processed on that system.

(2) System users will ensure that no unauthorized personnel are allowed to view sensitive unclassified or classified information while it is being processed.

(3) Diskettes on which information of continuing importance is stored will contain an appropriate security classification label and be controlled in accordance with the procedures outlined in paragraph 8 of this instruction. In addition, a duplicate copy of a diskette will be made each time its data content is changed.

(4) The security and disposal measures outlined in paragraph 7(o) of this instruction will be applied to all diskettes and hard drives which contain classified data.

(5) Appropriate classification labels will be affixed to the upper and lower edges of all classified listings. These markings may be automated or may be affixed manually.

(6) Data stored on network or local (installed in an AIS) hard drives will be routinely copied to tape (backed-up) in accordance with the specifications listed below. All tapes utilized for backup procedure will be managed in accordance with paragraph 9 of this instruction.

(a) All network drives will be backed-up daily.

(b) All local drives whose data content undergo frequent modification will be backed-up each working day. Otherwise, a full backup of the local drive will be accomplished at least weekly.

o. Magnetic Media Security and Disposal. A common misconception of uneducated computer users is that data stored on magnetic storage devices can be successfully removed by reformatting the media or by deleting the files in which the data is stored. While both procedures will prevent direct access to the data, neither procedure will totally remove the data and routines exist which can be used to reconstruct deleted files and/or reformatted drives. Accordingly, all MOMAG activities will apply the following security and disposal procedure to magnetic media:

1 NOV 1994

(1) No classified information will be stored on any fixed (non-removable) hard disk unless specifically authorized by COMOMAG.

(2) All diskettes and all hard drives on which classified information is stored will carry a Department of the Navy (DON) magnetic media label identifying the highest classification of data stored on the device. These include:

<u>TITLE</u>	<u>LABEL NUMBER</u>
Top Secret	SF706
Secret	SF707
Confidential	SF708
Classified	SF709
Unclassified	SF710
Data Descriptor	SF711

(3) Once utilized for classified storage at a given classification level, a diskette will not be reassigned for use at a lower classification level. If the diskette is defective or is no longer required, it will be destroyed by incineration or disintegration.

(4) No hard drive on which classified information has been stored will be reassigned for use at a lower classification level or released to any facility for reutilization unless a government approved data removal routine such as Norton Utilities' "WIPEINFO" is first used to declassify the disk.

(5) Defective hard drives on which classified information has been stored which cannot be forwarded to a cleared repair facility or which are considered non-repairable will be destroyed in accordance with procedures outlined in reference (j). Approved procedure is:

(a) Document the material destruction in accordance with requirements specified for the classification level;

(b) Remove the drive from the system unit, open the drive and remove the disk plates;

(c) Use a grinding wheel to totally remove the surface material from both sides of the plates or drench the plates in gasoline and ignite them or use a torch to burn the entire surface of the disk;

(d) Pulverize the plates with a sledge hammer;

(e) Dispose of the remains as unclassified waste.

p. Virus Protection. The introduction of computer viruses into the command's computer systems represents an ever

1 NOV 1994

increasing threat which can only be countered by a comprehensive virus prevention program. Accordingly, all MOMAG activities will implement the virus prevention countermeasures defined below. All incidents of virus infection will be reported in accordance with reference (f) as expanded by NAVELEXSECCEN 240243Z AUG 93. COMOMAG will be info addressee on all related official correspondence and message traffic.

(1) Computer virus awareness shall be emphasized in all AIS security briefs and training sessions. Training shall emphasize the fact that no current virus screening software ensures total virus protection and that anyone who knowingly violates virus protection policy shall be subject to disciplinary action.

(2) All AIS's will be equipped with anti-virus detection software. The software will be activated during the boot process and will only be deactivated to perform software installations or special disk maintenance tasks such as disk fix, disk compression and disk reorganization.

(3) No foreign diskettes (diskettes created on non-MOMAG AIS equipment) will be inserted into a MOMAG system until the ADPSO or his designated representative has performed a thorough virus screen on the disk and has approved its use. Diskettes generated by systems which have proven virus prevention measures in place may be exempt from this requirement by the CO/OIC.

(4) All data/software downloaded from a bulletin board will be downloaded to diskette and the diskette subsequently screened for computer viruses. Systems such as CAIMS, GATEGUARD, BUPERS ACCESS or other similar systems which have virus prevention measures in place may be exempt from this requirement by the CO/OIC.

8. Diskette management. All MOMAG activities will implement the following diskette management system to provide a means for identifying and locating information of continuing importance stored on diskettes. This procedure does not apply to copies of software distribution disks. Those disks will be tracked as part of the AIS inventory.

a. Where practical, information stored on diskettes will be grouped by SSIC in order that the SSIC can be used to identify both the diskette and the type of information stored on it. For example, correspondence with an SSIC of 1000 might be stored on a diskette labeled "SSIC 1000-1". If that diskette becomes full, a second diskette labeled "SSIC 1000-2" would be created.

b. When using SSIC's is not practical or when SSIC's do not apply to a general category of information stored on a

**1 NOV 1994**

diskette, a name which best describes the information shall be used (i.e. "MEMOS"). As in the case where an SSIC is used, the diskettes for the MEMOS category would be identified as "MEMOS-1", "MEMOS-2" , etc.

c. During diskette formatting procedures, the disk name will be assigned as the internal volume label.

d. All departments who utilize diskettes for data storage will maintain an inventory of their diskettes in a ledger or automated file. Those activities who have a network installed may track all command diskettes in a single data base. The following information will be maintained for each disk:

- (1) Department: (major key)(department name);
- (2) Disk ID: (minor key)(SSCI 1000-1, etc.);
- (3) Custodian: (custodian's name);
- (4) Location: (storage location);
- (5) Classification: (security classification);
- (6) Inventory Date: (last inventory date);
- (7) Inventoried By: (inspector's initials).

e. All departments utilizing diskettes for data storage will maintain a folder containing a directory listing for each diskette in inventory. The new directory listing for a diskette will be generated each time files are added to or deleted from the disk. Enclosure (10) is an example of the directory listing required and can be obtained in the following manner:

- (1) Place the diskette in disk drive A or B;
- (2) Place the system's printer on-line;
- (3) At the "C:\> " prompt, enter "Dir x: > prn"

where "x" is drive A: or B:.

f. Each department will conduct a quarterly physical inventory of diskettes including the following steps:

- (1) Verify all diskettes are present and that current directory listings match diskette contents;
- (2) Record the inventory in the inventory ledger or file;
- (3) Notify the ADPSO by memorandum (see enclosure (11)) that the inventory has been completed and of any discrepancies noted. The ADPSO will maintain copies of these memorandums for one year.



1 NOV 1984

9. Tape management. All MOMAG activities will implement the following tape management system to provide a means for identifying, locating and safeguarding magnetic tapes utilized by the command.

a. Each computer network and each AIS whose data content undergoes frequent change will be assigned eight tapes for back-up purposes. Four of these tapes will be utilized for the Monday through Thursday backup and will be labeled accordingly. The remaining four tapes will be labeled "1st and 5th Friday", "2nd Friday", "3rd Friday", and "4th Friday" respectively and will be used for weekly (Friday) back-ups on a rotational basis. This procedure will provide a four week data recovery window.

b. Each tape will be assigned a tape ID which includes the AIS ID plus a sequential number (i.e. OPS-01-1).

c. All daily backup tapes will be stored in a central on-site storage location which affords the best fire and security protection available. Ideally, a vault or similar storage facility should be utilized when available. No backup tapes are to be stored in the immediate area of the AIS whose data is contained on the tape.

d. Each CO/OIC will negotiate written off-site storage agreements with activities in their area where the latest weekly (Friday) backup tapes and all data archive tapes can be stored. ADPSO's will establish a weekly procedure whereby weekly save tapes are collected, recorded and forwarded to the off-site storage facility.

e. All departments who utilize magnetic tapes will maintain an inventory of their tapes in a ledger or automated file. Those activities who have a network installed may track all command tapes in a single data base. The following information will be maintained for each tape:

(1) Department: (major key) (department name);

(2) Tape ID: (minor key) (system ID+seq nr);

(3) Custodian: (custodian's name);

(4) Location: (storage location);

(5) Classification: (security classification);

(6) Inventory Date: (last inventory date);

(7) Inventoried By: (inspector's initials)

1 NOV 1994

f. Each department will conduct a quarterly physical inventory of its tapes including the following steps:

- (1) Verify that all tapes are accounted for;
- (2) Record the inventory in the inventory ledger or file;
- (3) Notify the ADPSO by memorandum (see enclosure (11)) that the inventory has been completed and of any discrepancies that were noted. The ADPSO will maintain copies of these memorandums for one year.

10. Personnel Qualification Standards (PQS). All personnel who utilize AIS equipment will be required to complete the PQS outlined in enclosure (12) before they are allowed to operate AIS equipment. The ADPSO or his designated representative will certify trainee qualifications by signing the PQS check-list as each requirement is completed. The PQS shall be entered into the member's training folder and forwarded with the individual upon his/her reassignment. Members who completed the PQS requirement at a previous command will not be required to requalify if their PQS sign off sheets were forwarded and they demonstrate competence in operating the equipment.

11. Hardware and Software Registration. All hardware and software warranty/registration cards shall be promptly filled out and mailed by COMOMAG as new purchases and/or upgrades are received. In addition, COMOMAG will maintain an inventory of all hardware and software issued to MOMAG activities and will verify its presence during Administrative and Material (ADMAT) inspections.

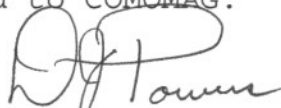
12. Hardware Maintenance. COs/OICs will conduct a survey of local military activities and civilian businesses to determine if local maintenance support is available for their AIS equipment. During the survey, emphasis will be placed on per incident support rather than blanket support agreements. If local support is not available, activities will report all AIS component failures to COMOMAG via FAX or Naval message. The report will identify the component, its model number, its serial number if applicable and a brief failure description. COMOMAG will then forward a replacement component via the fastest means possible and the defective component will be returned to COMOMAG for repair or replacement. If local support is available, a request to utilize the local source will be submitted to COMOMAG for approval. The request will include the following information:

- a. The support facility's name;
- b. Whether the facility is a civilian or military organization;
- c. A description of support options and their costs;

1 NOV 1994

d. An impact statement if the request where to be disapproved.

13. Action. CO's/OIC's will implement the conditions of this instruction upon receipt. Copies of local security procedures, contingency plans, AIS security violation reports and virus incident reports will be forwarded to COMOMAG.



D. J. POWERS

Distribution

COMOMAG/MOMAGINST 5216.1N

List II, Case A

COMINEWARCOM (N6)

1 NOV 1994

## DEFINITION OF TERMS

ACCREDITATION - A formal declaration by the Designated Approval Authority (DAA) that an AIS or computer network is approved to operate in a security environment which meets a specific technical security standard.

ACTIVITY AIS SECURITY PLAN (AAISSP) - An accreditation control document which outlines the scope and objectives of an activity's AIS security program by defining its organizational structure, staff responsibilities, security policy, current AIS environment and accreditation Plan of Action and Milestones.

AUTOMATED INFORMATION SYSTEM (AIS) - An assembly of computer hardware, software and/or firmware which may be used to collect, create, communicate, disseminate, process, print, store and retrieve data or information.

COMPUTER NETWORK - A group of AIS's which are physically linked together and which utilize special network hardware and software to share programs, data, printers and other computer resources.

COMPUTER VIRUS - Computer programs containing malicious logic which covertly replicates and attaches itself to valid program code and which when triggered, will take hostile action against the host computer system. Computer virus replication normally occurs during computer-to-computer communications and during magnetic media I/O operations.

CONTINGENCY PLAN - A plan of action which outlines emergency, backup and post recovery procedures required to ensure continued availability of critical AIS resources following a disaster or emergency situation.

COUNTERMEASURE - An action, device, procedure, technique or other measure which reduces the vulnerability of an AIS or computer network.

CLASS C2 FUNCTIONALITY - A Set of security measures which provide discretionary access control, memory clearing before reuse, individual accountability and audit trails for an AIS or computer network.

DESIGNATED APPROVAL AUTHORITY (DAA) - The official who is authorized to issue an accreditation statement which specifies that an AIS or computer network may operate in a security environment defined by a formal risk assessment process.

DATA BACK-UP - A procedure whereby information stored on magnetic disk is copied to tape or another disk to provide a means for recovering such information should it be lost or destroyed.

1 NOV 1994

MISSION CRITICAL APPLICATIONS - Applications which could unduly hinder or prevent an activity from meeting its mission objectives.

PASSWORD - A group of alpha, numeric and special characters which when associated with a user name provide a means for controlling access to an AIS/Computer network and the processes and information available on them.

PHYSICAL SECURITY - Those physical measures employed by an activity to safeguard equipment, facilities, material and documents against unauthorized access, espionage, sabotage, damage and theft. Physical security also includes measures designed to protect personnel.

RISK ASSESSMENT - An analysis of vulnerabilities and threats associated with an AIS or computer network which is conducted to determine the operational security requirements for such assets.

RISK MANAGEMENT - A process through which undesirable events can be identified, measured, controlled and prevented to effectively minimize their impact or frequency of occurrence.

SAFEGUARDS - Measures and/or controls implemented to protect and AIS/computer network and the information processed on them against loss or destruction.

SECURITY SURVEY - A survey of an AIS's security environment which is conducted as the first step in the Risk Assessment process. The survey identifies the AIS, its location and processing requirements, as well as vulnerabilities and threats associated with its use.

TELECOMMUNICATIONS - The transmission, emission, or reception of signs, signals, writings, images, sounds, or information of any nature by wire, radio, visual, or other electromagnetic systems.

TEMPEST - The study and control of spurious electronic signals emitted by AIS equipment.

TEMPEST VULNERABILITY ASSESSMENT AND INSTRUMENTED SURVEY REQUEST (TVAR) - A formal TEMPEST survey request submitted to Commander, Naval Security Group Command which identifies the AIS equipment concerned and defines the TEMPEST posture in which it operates.

TRUST LEVEL - The security level assigned to an AIS or computer network which identifies the level of protection its security features will provide.

1 NOV 1994

SAMPLE ABBREVIATED SYSTEM DECISION PAPER  
(ASDP)ABBREVIATED SYSTEM DECISION PAPER  
FOR  
MOBILE MINE ASSEMBLY GROUP AUTOMATION

ACTIVITY: Commander, Mobile Mine Assembly Group  
2536 Fourth St. Naval Station Annex  
N. Charleston, SC 29406-6171

POINT OF CONTACT: A. D. Hanna, GS-12, AV 563-6995, COMM  
(803) 743-6995

1. NEED. In an effort to reduce the paper products generated in DON, many publications, procedures and instructions are now being issued on CD-ROM. In addition, COMINELWARCOM has indicated that they intend to begin issuing Minefield Planning Folders on CD-ROM in the not too distant future. All MOMAG activities are currently equipped with one dual CD drive which is usually installed in their Supply Departments. These systems are frequently located some distance from other site departments which require CD-ROM support and make it extremely inconvenient if not impossible to obtain timely CD support. In addition, some applications such as the Navy's FED LOG system require multiple drives to operate efficiently. Accordingly, an urgent need now exists to purchase additional CD-ROM drives for the MOMAG activities.

2. PROPOSED SOLUTION. CD-ROM units are available via the Naval Supply System at reasonable cost. The required units would be procured through normal supply channels over a two year period. The schedule for ADP procurement and implementation is as follows:

- a. Abbreviated System Decision Paper approval: JUN 94
- b. Procurement and receipt of FY94 equipment: SEP 94
- c. Site installation: OCT 94
- d. Procurement and receipt of FY95 equipment: JUN 94
- e. Site installation: SEP 94

3. OTHER ALTERNATIVES CONSIDERED. There are no alternatives to CD-ROM equipment.



1 NOV 1994

4. COST AND BENEFITS.a. Cost. The projected five year costs are:

FY94 (11 units) \$6,512

FY95 (10 units) 5,920

TOTAL COSTS \$12,432

b. Benefits. The primary benefits to be derived from the proposed CD-ROM drives is the reduction in paper files which can be realized through the introduction of CD-ROM technology.5. INTERFACE CONSIDERATIONS. The recommended equipment is IBM compatible and will provide required compatibility with present and future DOD systems.6. FUNDING. No funding has been approved for the proposed procurement.7. ACQUISITION STRATEGY. All ADP equipment purchases will be reviewed by COMINELWARCOM Code N6. Required units will be purchased through the Naval Supply System.8. OTHER COMMENTS.a. Training. Training will be provided by tutorial packages included with the software.b. Security. Standard operating procedures which incorporate security safeguards for automated systems have been provided to each site. In addition, all site CO's are required to adhere to the accreditation requirements outlined in SECNAVINST 5239.2.c. Maintenance. The equipment recommended in this proposal is covered by a one year warranty. Following that period, maintenance support will be provided on a per case basis.9. JOINT SIGNATURE.FUNCTIONAL REQUIREMENT  
VALIDATED:\_\_\_\_\_  
REQUESTER\_\_\_\_\_  
DATEACQUISITION OF SYSTEM  
APPROVED:\_\_\_\_\_  
APPROVING AUTHORITY\_\_\_\_\_  
DATE

1 NOV 1994

## SAMPLE APPOINTMENT LETTERS

From: Commanding Officer/Officer in Charge, MOMAG \_\_\_\_\_  
To: APPOINTEE'S RANK, NAME, SSN

Subj: APPOINTMENT AS ADP SECURITY OFFICER

Ref: (a) SECNAVINST 5239.2  
(b) OPNAVINST 5239.1A  
(c) OPNAVINST C5510.93E  
(d) CINCLANTFLTINST 5239.1  
(e) COMOMAG/MOMAGINST 5230.1C  
(f) COMMAND SECURITY INSTRUCTION

1. In accordance with reference (a), you are hereby designated as the ADP Security Officer for this command. You will thoroughly familiarize yourself with references (a) through (f). Your duties include:

a. Developing, implementing and maintaining the command AIS Security Program.

b. Coordinating with the command security manager on matters concerning ADP security.

c. Ensuring that Terminal Area Security Officers (TASO) and Network Security Officers (NSO) are appointed in writing where applicable.

d. Developing, testing, implementing and maintaining command AIS contingency plans.

e. Coordinate requests for TEMPEST clearance in accordance with reference (e).

f. Ensuring accreditation support documentation is developed and maintained including Risk Assessment, Security Test & Evaluation (ST&E), and a contingency plan.

g. Developing and implementing a comprehensive command anti-virus familiarization and screening program.

h. Developing, implementing and maintaining a command AIS user training and Personal Qualification Standard (PQS) program.

i. Ensuring all security incidents or violations are investigated, documented, and reported to proper authority.

j. Documenting and reporting incidents of virus infections to the CO/OIC.

1 NOV 1994

k. Conducting periodic checks to ensure ADP security requirements in reference (e) and (f) are met.

l. Maintaining a current inventory of command AIS hardware and software.

m. Developing additional AIS requirements documentation in accordance with enclosure (2) to reference (e).

Commanding Officer/Officer in Charge

1 NOV 1994

From: Commanding Officer/Officer in Charge, MOMAG \_\_\_\_\_  
To: APPOINTEE'S RANK, NAME, SSN

Subj: APPOINTMENT AS TERMINAL AREA SECURITY OFFICER

Ref: (a) SECNAVINST 5239.2  
(b) OPNAVINST 5239.1A  
(c) OPNAVINST C5510.93E  
(d) HOST COMMAND SECURITY INSTRUCTION  
(e) COMOMAG/MOMAGINST 5230.1C  
(f) COMMAND SECURITY INSTRUCTION

1. In accordance with reference (a), you are hereby designated as the Terminal Security Officer for *TERMINAL-ID*. You will thoroughly familiarize yourself with references (a) through (f). Your duties include:

a. Preparing and forwarding user access requests to host activities.

b. Issuing user passwords forwarded by the host activity and submitting required reports.

c. Informing the ADPSO and terminal users of host activity security requirements.

d. Ensuring security measures specified by the host activity are adhered to during remote terminal sessions.

e. Reporting all breaches of terminal security to the host activity and to the ADPSO.

Commanding Officer/Officer in Charge

1 NOV 1994

From: Commanding Officer/Officer in Charge, MOMAG \_\_\_\_\_  
To: APPOINTEE'S RANK, NAME, SSN

Subj: APPOINTMENT AS NETWORK SECURITY OFFICER

Ref: (a) SECNAVINST 5239.2  
(b) OPNAVINST 5239.1A  
(c) OPNAVINST C5510.93E  
(d) COMOMAG/MOMAGINST 5230.1C  
(e) COMMAND SECURITY INSTRUCTION

1. In accordance with reference (a), you are hereby designated as the Network Security Officer for the command's computer network. You will thoroughly familiarize yourself with references (a) through (e). Your duties include:

- a. Administering the command's computer network.
- b. Assisting the ADPSO in administering the Command AIS Security Program as it pertains to the command's computer network.
- c. Developing, implementing and maintaining a network user training and Personal Qualification Standard (PQS) program for the command.
- d. Assisting the ADP Security Office (ADPSO) in completing all AIS accreditation requirements for the command's computer network.
- e. Reporting all network security violations to the ADPSO.

Commanding Officer/Officer in Charge

1 NOV 1994

## ADP SECURITY TRAINING SOURCES

<u>ACTIVITY</u>	<u>POC</u>	<u>PHONE</u>
NCTS Naval Air Station Jacksonville, FL	John Free Code N943	(904)779-6172 DSN 942-5351
NCTAMS, Eastern Pacific Pearl Harbor, HI	Alan Saka	(808)474-0711
NCTS San Diego San Diego, CA	Guy Casciola Code N823	(619)545-8628 DSN 735-8628
NARDAC San Francisco NAS Alameda, CA	Joyce Ferris Code 62	(415)263-5313 DSN 993-5313
NCTS Washington Washington Navy Yard Washington, DC	Jerome Short Code 512	(202)433-4106 DSN 288-4106



1 NOV 1994

## SAMPLE ACCREDITATION LETTER

From: Commanding Officer/Officer in Charge, MOMAG \_\_\_\_\_  
To: ADP Security Officer

Subj: LETTER OF ACCREDITATION

Ref: (a) OPNAVINST 5239.1A  
(b) COMOMAGINST 5230.1C  
(c) COMMAND SECURITY INSTRUCTION

1. In accordance with references (a) through (c), the following ADP systems within this command have a completed risk assessment, Security Test and Evaluation (ST&E) and contingency plan and are fully accredited to operate within this command:

\*\*\*LIST SYSTEMS OR SYSTEM GROUPS \*\*\*

Commanding Officer/Officer in Charge

1 NOV 1994

AUTOMATED INFORMATION SYSTEM (AIS)  
CONTINGENCY PLAN  
FOR

Commander, Mobile Mine Assembly Group (COMOMAG)  
Charleston, SC

## 1.0 INTRODUCTION

COMOMAG has become increasingly dependent upon AIS systems to perform its mission. The Department of the Navy (DON) AIS Security Program mandates that an active Risk Management Program be implemented by all activities who rely upon AIS services. Included in the Risk Management Program is the requirement to develop a contingency plan which provides reasonable support for essential procedures if an unforeseen AIS service disruption should occur.

### 1.1 Purpose

This document provides essential contingency guidance in terms of preparatory, emergency reaction, backup processing and service restoration activities following a total or partial disruption of Micro Computer services within the command.

### 1.2 Objectives

This plan is designed to meet the following contingency objectives.

- a. To provide continued AIS support required by COMOMAG to meet its mission objectives.
- b. To document specific actions to be taken during and after a disruption of AIS services.
- c. To provide the resources and procedures required to restore normal AIS services.

### 1.3 Scope

This plan defines contingency procedures for that micro computer equipment installed at the COMOMAG Headquarters located at 2536 Fourth St, NAVSTA Annex, N. Charleston, SC. An evaluation of all applications has been conducted and workload priorities have been established.

1 NOV 1994

## 2.0 PLANNING CONSIDERATIONS

### 2.1 Environmental Assessment

Potential threats to and their impact upon COMOMAG micro computer assets were evaluated and where possible, cost effective safeguards against such threats have been identified and implemented. A prioritized list of residual threats was used to develop those contingency actions outlined in the plan and the potential losses associated with these threats were used to compute the cost effectiveness of contingency reactions listed. For purposes of this plan, mission essential systems for which no backup support can be identified will tolerate a down time of not more than 1 working day. Non-mission essential systems will tolerate reasonable down time required to repair the system. The continued effectiveness of this plan will be validated by risk analyses conducted in the future.

### 2.2 Workload Evaluation and Prioritization

The Critical Processing List provided in Appendix A, outlines the priorities assigned to specific tasks during implementation of this plan. The list was compiled from data submitted by all major departments and is subject to change. While this plan is designed to limit the impact of AIS disruptions to tolerable limits, some services must necessarily be reduced when processing capability is lost.

### 2.3 Commitment to Support

COMOMAG and its staff are committed to the contingency planning process. COMOMAG's Chief Staff Officer is designated as Contingency Task Team Leader and has the authority to coordinate the activities of other team members.

## 3.0 RESPONSIBILITIES

COMOMAG's Contingency Reaction Team Organization Chart is provided in Appendix B. Individual responsibilities for each functional area are established and approved by the Commanding Officer and are listed in the Contingency Personnel Control List provided in Appendix B.

## 4.0 CONTINGENCY PLAN STRUCTURE

The Contingency Reaction Plan outlined in Appendix C addresses two specific types of actions. The first prepares the command for a contingency situation by detailing requirements for generating backup copies of all software, data and documentation utilized within the command and storing those backups in various

1 NOV 1994

secure locations. It will also identify equipment repair sources which will be utilized in the event a hardware failure should occur. The second identifies those steps which will be taken during a contingency situation. This section is subdivided into three sections. They are:

a. Emergency Response. Emergency response procedures outline those actions to be taken immediately following a contingency situation. Contingency situations which can be recovered from quickly which do not require movement to alternate facilities are included in this area (e.g. minor fires, short term power failures, etc).

b. Backup Processing. Backup processing strategy details those actions required to respond to a partial loss of on-site processing and/or to transfer processing to a backup processing facility when command AIS equipment will be unavailable for an extended period of time.

c. Recovery. Recovery strategy defines those actions required to restore normal operations following a contingency.

5.0 Mutual Backup Support Agreement. A mutual backup support agreement with MOMAG Unit 11 has been established which provides for mutual support and assistance in recovering from a catastrophe which effects either party. A copy of the formal agreement is included in Appendix D.

## 6.0 CHANGE CONTROL/PLAN DISRUPTION

6.1 Change Control. The command's ADP Coordinator, Code N01F, is responsible for posting changes to this document. Recorded changes shall include change number, date of change, purpose of change and other relevant information. The Change Control Log shall be maintained as Appendix E to this plan.

6.2 Plan Distribution. This contingency plan is approved by the Commanding Officer. A copy of the plan is maintained in the off-site backup storage facility along with all other required backup resources. Copies of this plan will be distributed as listed below:

Individual/Activity Name	Telephone Number
<u>COMINNEWARCOM, Code N62</u>	<u>DSN 861-4891</u>
<u>MOMAG UNIT 11</u>	<u>(803)743-6040</u>

1 NOV 1994

## APPENDIX A

## CRITICAL PROCESSING LIST

1. INTRODUCTION. This critical processing list is organized by department and identifies those processes which are considered crucial to each department meeting its mission objectives.

2. ADMIN DEPARTMENT (N1)

<u>PROCESS</u>	<u>PRIORITY</u>
MESSAGE TRAFFIC (MDU/MTF)	1
WORD PROCESSING (Microsoft Word)	2

3. OPERATIONS DEPARTMENT (N3)

<u>PROCESS</u>	<u>PRIORITY</u>
WORD PROCESSING (Microsoft Word)	1
DATA BASE MANAGEMENT (First Choice)	2
PROJECT MANAGEMENT	3
PRESENTATIONS (Harvard Graphics, Scanner)	4

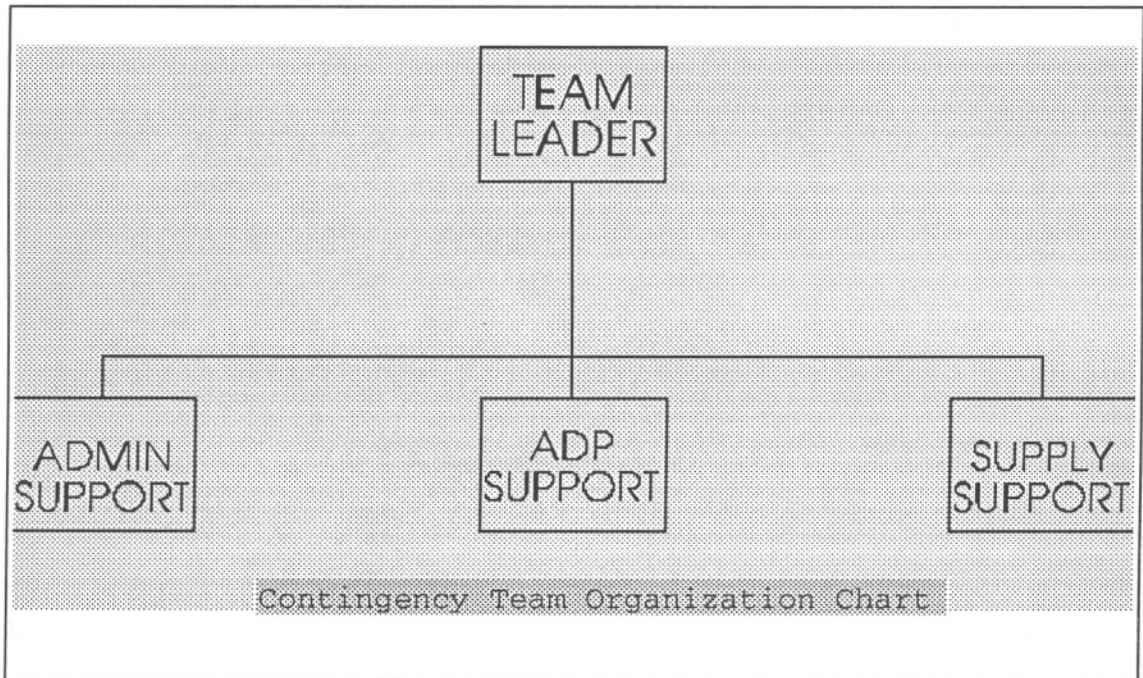
4. SUPPLY DEPARTMENT (N4)

<u>PROCESS</u>	<u>PRIORITY</u>
FAADCLANT UPDATE (UNISCOPE, MODEM, MUX)	1
WORD PROCESSING (Microsoft Word)	2
FUNDS STATUS (BUDGET, WINDOWS 3.1, EXCEL)	3

1 NOV 1994

APPENDIX B  
CONTINGENCY REACTION TEAM ORGANIZATION

1. TEAM ORGANIZATION CHART



2. CONTINGENCY PERSONNEL CONTROL LIST

- a. Team Leader- Chief Staff Officer, Code 01
- b. Admin Support- Administration Officer, Code N1
- c. ADP Support- ADP Coordinator, Code N01F
- d. Supply Support- Supply Officer, Code N4

3. RESPONSIBILITIES

a. Team Leader. The Team Leader will decide when a contingency situation exists and will specify which contingency actions are to be implemented. The team leader will act as primary liaison with higher authority and with other activities identified in this plan. While those actions outlined in this



1 NOV 1994

plan will provide primary guidance in dealing with a contingency, the Team Leader may deviate from them when circumstance justifies it. In addition, the Team Leader may delegate some or all of his responsibility to other members of the team.

b. Administrative Support. The Administrative Support member will ensure that all correspondence, message and clearance processing required to support this plan are provided for in a timely manner. He/she, in consultation with Code N01F, will establish an administration Standard Operating Procedure (SOP) for supporting this plan and will ensure that responsible administrative personnel have been indoctrinated in that procedure. As a minimum, this plan shall include:

(1) Procedures for identifying requirements for and forwarding of personnel security clearances.

(2) Procedures for notifying interested commands in the event AIS operations must be relocated.

(3) Procedures for acquiring STU III telephones for secure data transmissions.

(4) Security procedures to be followed during AIS relocation periods.

(5) Routing procedures for command correspondence during AIS relocation periods.

c. ADP Support. The ADP Support member will serve as primary technical advisor to the Team Leader. He/she is responsible for developing and maintaining the AIS Contingency Plan, for implementing and monitoring the procedures outlined in the plan, for assisting other team members in completing their responsibilities and for assisting other departments in preparing their contingency plan SOPs. He/she will negotiate the terms of mutual support agreements and will develop agreement drafts. He/she will conduct periodic tests of contingency procedures and will report the results of such tests to the Team Leader.

d. Supply Support. The Supply Support member will ensure that adequate funding for contingency support is identified in the COMOMAG budget and will define the procedure required to request any emergency funding identified in Appendix C. He/she will ensure that sources for micro computer maintenance support have been identified and that procedures for obtaining such services are in place. In addition, he/she will ensure that appropriate sources and procedures for obtaining other AIS materials required to support this plan are available.

1 NOV 1994

APPENDIX C  
AIS CONTINGENCY REACTION PLAN

1. OVERVIEW. This Contingency Reaction Plan identifies two types of actions which together will provide reasonable assurance that COMOMAG will have adequate AIS capability in place to support its most crucial processing requirements. The first of these outlines contingency preparation procedures which will provide those basis items required to recover from an AIS casualty. The second outlines those actions to be taken in the event a casualty should occur and defines three specific responses. These include an Emergency Response, a Backup Processing Response and a Recovery Response.

2. CONTINGENCY PREPARATION.

a. Hardware/Software - Code N01F will ensure that:

(1) All software purchased for the command is properly registered with the vender;

(2) Copies of locally developed programs are copied to diskette;

(3) A complete list of all software utilized by the command is maintained and stored at MOMAG Unit ELEVEN;

(4) Working copies of original diskettes are made and utilized to install the product;

(5) One complete package (software and documentation) of all software utilized by the command is stored at MOMAG Unit ELEVEN;

(6) One copy of software program diskettes are stored in the Headquarter's vault located in room 212;

(7) One copy of software documentation is distributed to each department that uses it;

(8) All remaining copies of software diskettes and documentation are stored in storage cabinets located in Headquarters room 119;

(9) A list which identifies the replacement costs and procurement sources for all AIS hardware and software utilized by the command is compiled and a copy is stored in the Headquarters vault and at MOMAG Unit ELEVEN; and

1 NOV 1994

(11) That MOMAG Unit ELEVEN is provided a copy of COMOMAG personnel security clearances.

b. Tape Backup. All software and data contained on micro computer systems located in the COMOMAG Headquarters building will be copied to tape on a regular basis. **A FILE VERIFICATION PASS WILL BE PERFORMED** each time tape backups are made. All tapes will contain appropriate classification labels. The following specifics are provided:

(1) Micro computers which are used primarily as workstations for the Novell Network and on whom user data is not normally stored will be backed up to tape **each Friday** and the tape forwarded to designated storage. All other Micro's will be backed up to tape each time the data on their hard drive is changed. COMOMAG's designated storage is the command vault.

(2) Code N01F will perform a complete NOVELL file server backup to tape **at the end of each work day**. Code N01F will ensure that the server backup tapes are forwarded to the command vault for storage.

(3) Each Monday, the command Radioman will collect all save tapes generated during the previous Friday's backup process and forward them to MOMAG Unit ELEVEN for storage. In addition, he/she will retrieve the tapes stored at MOMAG Unit ELEVEN the previous week and distribute them to the appropriate departments.

c. Equipment Protection. Plastic covers will be provided for all command micro computers and printers. These covers will be placed on the equipment at the end of each work day and in the event of fire, prior to evacuating the building. All system users will ensure that the RFI filtering devices and the surge protection devices provided for their systems are utilized at all times.

d. Maintenance Support. All, except two, of the workstations utilized at COMOMAG were purchased from "PX of Charleston." The NOVELL file server and the NOVELL software were purchased from "Computer Products of Charleston." Both companies provide hardware and software support for their respective systems and COMOMAG has Blanket Purchase Agreements (BPA) in place with each. In addition, COMOMAG has a standing work request for Zenith 248 maintenance support with the Naval Aviation Depot, MCAS, Cherry Point, NC. All UNISYS equipment will be supported through standing DON maintenance support agreements with UNISYS Corp. In addition, COMOMAG will strive to maintain a reasonable on-board inventory of spare components for its systems.

1 NOV 1994

## 2. CONTINGENCY ACTION.

a. Emergency Response. These procedures outline actions to be taken when minor disruptions of a temporary nature occur which will not require relocation to a backup processing facility.

(1) Power Failure. In the event a short term power failure should occur, all AIS equipment will be powered off until electrical power has been restored and is considered stable. The single exception is the NOVELL file server which is protected by a backup power supply that automatically powers the server down when emergency power has been exhausted.

(2) Workstation failure. In the event a hardware component should fail, the user will notify Code N01F who will attempt to correct the problem. If the problem cannot be corrected, Code N01F will arrange to have the system repaired and when necessary, will arrange for alternative in-house computer support. The following specifics apply:

(a) Radioman's system. If the Radioman's system fails and cannot be repaired within four hours, a system with a DataPort drive will be temporally relocated to the administrative spaces and the processing normally performed on the relocated system reassigned to another workstation. The systems identified as possible replacements in the order of precedence are Admin System-3, Admin System-4, Admin System-2, Admin System-1 and CO-Secretary-1.

(b) Any network workstation. Network applications are accessible from any workstation and emergency scheduling for required computer time can be easily arranged. The exception to this rule is the scanner located in room 209. Access to this equipment is not considered crucial. If data recovery is required, Code N01F will recover the data from the appropriate system backup tapes.

(c) Supply System-3. The hardware and software required to support the FAADCLANT data link is duplicated on the Supply System-4. If both systems should be lost, the hardware and software components required would be removed and installed in a substitute system until appropriate repairs can be affected.

(d) Workstation Hard Drive failures. Code N01F will replace defective workstation hard drives and will utilize the latest backup tapes to restore system and user files.

(3) NOVELL File Server. Disk mirroring has been implemented on COMOMAG's file server. Should the primary disk fail, the network will continue to operate until it can be downed temporally to correct the problem. Should a total server failure

1 NOV 1994

occur, all workstation disk drives have sufficient capacity to load Microsoft Windows and Microsoft Office to provide temporary backup processing until the server can be restored. Code N01F will provide temporary working copies of required network files from server backup tapes upon request. Printing support will be provided by temporarily attaching command printers to selected systems.

b. Backup processing. These procedures outline actions to be taken when major disruptions of AIS services or when relocation to a backup processing facility is required. Emergency responses listed above will be implemented where applicable. In addition, the actions listed here will be implemented as required.

(1) Power Failure Headquarters Building. In the event a power outage will extend beyond a tolerable limit determined by COMOMAG and power is available at MOMAG Unit ELEVEN, arrangements will be made to establish a mini network consisting of a single file server and six workstations in the MOMAG Unit ELEVEN Conference Room. All documentation required to support the critical processing listed on the Critical Processing List will be collected and transported with the hardware. If power is not available at MOMAG Unit ELEVEN, Code N01F will establish a mini network in room 105 using portable generator power.

(2) Loss of Headquarters facility. In the event all or part of the Headquarters facility is lost, Code N01F will evaluate the damage to the command's AIS assets and develop a proposal to restore a partial AIS capability as described under power failures. In addition, the following actions will apply:

(a) Code N01F will retrieve any backup tapes and software documentation required to restore systems from in-house storage or from the MOMAG Unit ELEVEN backup site.

(b) Code N01F will compile a list of equipment and software lost during the event and submit a report to the Supply Officer which identifies the replacement costs and procurement sources for lost items.

(c) The Supply Officer will prepare emergency requisitions for required materials.

(d) The Supply Officer will prepare and submit an emergency funding request to COMINELWARCOM (Code N4/6) to cover replacement costs for lost items and will requisition required replacements.

c. Recovery. Following a contingency which required relocation, the Team Leader will establish a date and time AIS

1 NOV 1994

processing will be terminated at the backup site. Prior to that date, Code N01F in conjunction with the contingency team will procure replacement AIS equipment if required and will establish at a minimum, a temporary stand alone capability for each department. Full restoration of AIS services will be completed as replacement hardware and software becomes available. Once full processing has been restored, Code N01F will ensure that all contingency preparation actions listed in this plan are reinstated.



1 NOV 1994

## ACCESS WARNING MESSAGE

\* \* \* \* \* \*WARNING\* \* \* \* \*

THIS IS A DOD INTEREST COMPUTER SYSTEM (DOD ICE)

Use of this or any other DOD Interest Computer System (DOD ICE) constitutes consent to monitoring at all times.

All DOD ICE and related equipment are intended for the communication, transmission, processing, and storage of official U.S. Government or authorized information only. All DOD ICE are subject to monitoring at all times to ensure proper functioning of equipment and systems, including security devices and systems, to prevent unauthorized use and violations of statutes and security regulations, to deter criminal activity, and for similar purposes.

Any user of a DOD ICE should be aware that any information placed on the system is subject to monitoring and NOT subject to any expectation of privacy. If monitoring of this or any other DOD ICE reveals possible violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring of this or any other DOD ICE reveals violations of security regulations or unauthorized use, employees who violate security regulations or make unauthorized use of DOD ICE are subject to appropriate disciplinary action.

USE OF THIS OR ANY OTHER DOD ICE CONSTITUTES CONSENT TO  
MONITORING



1 NOV 1994

## PC MAINTENANCE REQUIREMENT CARD (MRC)

Equipment Nomenclature: Zenith 248 and Unisys Computer systems	Frequency: Monthly
Maintenance Required: Clean and inspect Z248 and Unisys computer systems	Personnel Requirement: One E4 or E5
Safety Precautions: Secure system Power and disconnect CPU and Monitor power cables	Time Estimate: 1 Man Hour
Tools, Equipment, Supplies: 1. Cleaner, general purpose 7930-00-068-1699 2. Cleaner, Glass 7930-00-664-6910 3. Towel, cleaning (3) 7930-00-634-2408 4. Alcohol, Isopropyl 6505-00-261-7256 5. Screwdriver, phillips #2 5120-00-542-3438 6. Brush, paint, 1 inch (new/unused) 8020-00-263-3866 7. Applicator, disposable, cotton tipped, wood 6515-01-234-6838 8. Cleaner, Vacuum 9. Attachment, crevice tool, plastic, vacuum 10. Cleaning Kit, 5 1/4 inch floppy drive 11. Cleaning Kit, 3 1/2 inch floppy drive (Unisys only) 12. Z248 PC Series Computer Owner's manual (Z248 only) 13. PW2 Advantage Personal Workstation Installation Guide (Unisys only)	
Procedure: NOTE 1. Do not spray detergent directly on computer, monitor or keyboard. 2. Do not clean monitor with general purpose cleaner.  1. Clean and inspect CPU, monitor and keyboard. a. Apply general purpose cleaner to cleaning cloth. b. Remove all dust, dirt and grease from surface of CPU, monitor, keyboard covers and keyboard keys. c. Clean monitor screen with glass cleaner with clean, lint free cloth d. Use paint brush to clean dust from between keyboard keys. e. Inspect data cables for damage or loose connections and replace as required. 2. Clean CPU interior. a. Ensure CPU is powered down and all power cords are disconnected. b. Referencing the System's Owner's manual, remove the CPU cover. c. Periodically touch the surface of the system's power supply to release static charge buildup. d. Using the 1 inch paint brush, the vacuum and the plastic crevice tool, carefully vacuum all dust and dirt from system interior and power supply. DO NOT FORCE crevice tool between installed boards. DO NOT ALLOW metal vacuum parts to contact installed boards or system components. e. If excessive dust buildup between disk drives cannot be cleared, make note of the position of the RED stripe on each data cable, disconnect all data and power cables and vacuum the drives. Ensure all data and power cables are reinstalled in their original positions.	

1 NOV 1994

Equipment Nomenclature:  
Zenith 248 and Unisys Computer  
systems

## CONTINUATION SHEET

## Procedure: (continued)

- f. (2248 only) Using the alcohol and cotton applicators, clean the tape unit read/write head and drive mechanism.
  - g. Check interior for broken or frayed cables or wires. Have defective items replaced.
  - h. Check interior for broken or scorched components. Arrange for defective components to be replaced.
  - i. Referencing the system's Owner's manual, replace the CPU cover.
  - j. Reconnect all cables to CPU and monitor.
  - k. Turn equipment on.
  - l. If equipment fails to reboot, ensure all exterior/interior data cables were reinstalled correctly. If the problem cannot be corrected, arrange for maintenance service.
3. Clean Floppy drives.
- a. Using the 5 1/4 and 3 1/2 (Unisys only) disk drive cleaning kits, clean the systems floppy drives in accordance with kit instructions
4. Clean tape backup unit. (Unisys only)
- a. Using the mini data cartridge cleaning kit, clean the UNISYS tape backup unit in accordance with kit instructions.

1 NOV 1994

## PRINTER MAINTENANCE REQUIREMENT CARD (MRC)

Equipment Nomenclature: Alps 2000 Dot Matrix and NEC P6300 Dot Matrix printers	Frequency: Quarterly
Maintenance Required: Clean and inspect Alps 2000 and NEC P6300 printers	Personnel Requirement: One E4 or E5
Safety Precautions: Secure Printer Power	Time Estimate:
Tools, Equipment, Supplies: 1. Cleaner, general purpose 7930-00-068-1699 2. Cleaner, Platen 3. Towel, cleaning (3) 7930-00-634-2408 4. Alcohol, Isopropyl 6505-00-261-7256 5. Brush, paint, 1 inch (new/unused) 8020-00-263-3866 6. Cleaner, Vacuum 7. Attachment, crevice tool, plastic, vacuum	
Procedure: 1. Clean and inspect Printer exterior. a. Apply general purpose cleaner to cleaning cloth. b. Remove all dust, dirt and grease from printer cover. c. Inspect data cable for damage or loose connections. Replace as required. 2. Clean and inspect printer interior. a. Remove Printer access cover. b. Remove printer ribbon. c. (NEC only) Remove and inspect print head 1- release retained clips on each side of print head and lift the print head straight up. 2- remove all lint, paper and excess ink from print head. d. Pull paper bail away from platen. e. Moisten cleaning cloth with platen cleaner or Isopropyl alcohol and clean platen and cradle roller. Discard cloth when finished. f. Using the 1 inch paint brush, the vacuum and the plastic crevice tool carefully vacuum the printer interior. DO NOT FORCE the tool into narrow openings. DO NOT ALLOW metal vacuum parts to contact installed boards or printer components. g. Moisten another cleaning cloth with alcohol and wipe down accessible interior surfaces. h. Inspect print head drive belt for missing teeth or cracking. Submit printer for maintenance if required. i. Inspect interior for broken or frayed wires or cables. Submit for maintenance if required. j. (NEC only) Replace print head by inserting print head contacts in head slot and pressing straight down until the head snaps into place. Reseat the retainer clips. k. Replace printer ribbon. l. Replace printer cover.	

1 NOV 1994

Equipment Nomenclature: Epson Action Laser II	Frequency: Quarterly
Maintenance Required: Clean and inspect Action Laser II	Personnel Requirement: One E4 or E5
Safety Precautions: Secure Printer Power	Time Estimate:
<p>Tools, Equipment, Supplies:</p> <ol style="list-style-type: none"> <li>1. Cleaner, general purpose 7930-00-068-1699</li> <li>2. Towel, cleaning (3) 7930-00-634-2408</li> <li>3. Brush, paint, 1 inch (new/unused) 8020-00-263-3866</li> <li>4. Cleaner, Vacuum</li> <li>5. Attachment, crevice tool, plastic, vacuum</li> </ol>	
<p>Procedure:</p> <ol style="list-style-type: none"> <li>1. Clean and inspect Printer exterior. <ol style="list-style-type: none"> <li>a. Apply general purpose cleaner to cleaning cloth.</li> <li>b. Remove all dust, dirt and grease from printer cover.</li> <li>c. Inspect data cable for damage or loose connections. Replace as required.</li> </ol> </li> <li>2. Clean and inspect printer interior. <ol style="list-style-type: none"> <li>a. Open Printer access cover.</li> <li>b. Remove toner cartridge.</li> <li>c. Remove Photo Conductor unit</li> <li>d. Using the 1 inch paint brush, the vacuum and the plastic crevice tool carefully vacuum the printer interior. DO NOT FORCE the tool into narrow openings. DO NOT ALLOW metal vacuum parts to contact installed boards or printer components.</li> <li>e. Moisten another cleaning cloth with cleaner and wipe down accessible interior surfaces. Make sure the interior is dry before the photo conductor unit and toner cartridge are replaced.</li> <li>f. Inspect interior for broken or frayed components. Submit for maintenance if required.</li> <li>g. Replace Photo conductor unit. Follow the instructions on page 6-10 of the Owner's manual to clean the Unit's Charger Wire.</li> <li>h. Replace toner cartridge.</li> <li>i. Close printer cover.</li> </ol> </li> </ol>	

1 NOV 1994

## SAMPLE DISKETTE DIRECTORY LISTING

C:\&gt;DIR A:

Volume in Drive A is SECURITY01  
Volume Serial Number is 425F-0FD2  
Directory of A:\

INSTRUCT	DOC	10008	11-07-91	9:57a
ACCRED	DOC	1258	11-06-91	9:49a
ADPSP	DOC	8790	10-23-91	10:26a
AAS	DOC	6821	10-23-91	2:26p
CONTING	DOC	3710	11-06-91	2:09p
SOPS	DOC	10833	10-30-91	2:08p
README	DOC	5048	11-06-91	1:11p
INTERIM	DOC	1436	11-06-91	9:46a
RISKASS	DOC	18430	10-30-91	9:43a
ST&E	DOC	12260	11-06-91	1:09p
APPOINT	DOC	2474	11-07-91	9:52a

11 file(s) 81068 bytes  
277504 bytes free

C:\&gt;

1 NOV 1994

SAMPLE DISKETTE/TAPE INVENTORY NOTIFICATION MEMORANDUM

From: Department  
To: ADPSO

Subj: QUARTERLY DISKETTE/TAPE INVENTORY

Ref: (a) COMOMAG/MOMAGINST 5230.1C

1. In accordance with reference (a), the quarterly diskette/tape inventory was completed. No discrepancies/The following discrepancies were noted.

Department Head Signature

1 NOV 1994

## PERSONAL COMPUTER OPERATOR PQS

OVERVIEW. The training program outlined below identifies the basic AIS training each computer user will be required to complete before they are considered qualified to operate AIS equipment. Items I through IV provide a comprehensive overview of personal computers, the MS-DOS operating system and AIS security and will be considered mandatory for all users. Items V through IX are job specific and should be completed by those users whose job assignments require it. Once users have completed the mandatory training, an entry to that affect will be placed in their training folder. Users whose training folders indicate that mandatory training was completed during a previous assignment and who demonstrate competence in utilizing AIS equipment **WILL NOT BE** required to repeat the training. Site COs/OICs will ensure that similar PQS requirements are provided for personnel responsible for executing the SCAAIR and BATS programs, that qualified QPOs are identified to support the PQS program, that AIS security briefs are provided to all users within 30 days of their reporting onboard and that annual AIS security training is provided for all hands.

## I. Security Instructions

- A. Read SECNAVINST 5239.1B QPO\_\_\_\_\_
- B. Read COMOMAG/MOMAGINST 5230.1C QPO\_\_\_\_\_

## II. Introduction to PC (Mandatory)

## A. Instruction

1. Watch video entitled "Introduction to PC Computers." QPO\_\_\_\_\_
2. Complete tasks defined in the LEARN program contained on the "Introduction to PC Computers Diskette." QPO\_\_\_\_\_

## B. PQS

1. Identify and explain the function of the following major components:

- (a) CPU QPO\_\_\_\_\_



1 NOV 1994

- (b) CRT (monitor) QPO\_\_\_\_\_
- (c) Keyboard QPO\_\_\_\_\_
- (d) Floppy disk drives QPO\_\_\_\_\_
- (e) Hard disk drive QPO\_\_\_\_\_
- (f) Printer QPO\_\_\_\_\_
- (g) Backup tape drive QPO\_\_\_\_\_
- 2. Define the term RAM. QPO\_\_\_\_\_
- 3. Define the term conventional memory. QPO\_\_\_\_\_
- 4. Define the term extended memory. QPO\_\_\_\_\_
- 5. Define how RAM differs from disk storage. QPO\_\_\_\_\_
- 6. Demonstrate the method for determining the storage capacity of disk drives A and C. QPO\_\_\_\_\_
- 9. Describe the difference between a Dot Matrix and a Laser Printer. QPO\_\_\_\_\_
- 10. Identify the printer port. QPO\_\_\_\_\_
- 11. Identify the COM1 and COM2 ports. QPO\_\_\_\_\_
- 12. Identify the video port. QPO\_\_\_\_\_

### III. Introduction to Disk Operating System (DOS) (Mandatory)

#### A. Instruction

- 1. Watch video entitled "Introduction to DOS." QPO\_\_\_\_\_
- 2. Complete tasks defined in the LEARN program contained on the "Introduction to DOS Diskette." QPO\_\_\_\_\_
- 3. Complete Computer Based Instruction course "Professor DOS" lessons A (How to use Professor DOS), F (Advanced DOS commands), and G (Using a hard disk) QPO\_\_\_\_\_

#### B. PQS

- 1. Define what MS-DOS is. QPO\_\_\_\_\_

(PAGE )

1 NOV 1994

2. Describe how MS-DOS differs from applications software. QPO\_\_\_\_\_
3. Describe how DOS identifies floppy and hard disk drives. QPO\_\_\_\_\_
4. Define the term DOS DIRECTORY. QPO\_\_\_\_\_
5. Define the term ROOT DIRECTORY. QPO\_\_\_\_\_
6. Define how DOS identifies the ROOT DIRECTORY on the first hard drive installed in a system. QPO\_\_\_\_\_
7. Define the term DOS FILE. QPO\_\_\_\_\_
8. Name the two parts of a file name. QPO\_\_\_\_\_
9. Define the term FILE PATH. QPO\_\_\_\_\_
10. Which DOS command creates a directory? QPO\_\_\_\_\_
11. Which DOS command removes a directory from the disk drive? QPO\_\_\_\_\_
12. Demonstrate the procedure required to change the CURRENT directory. QPO\_\_\_\_\_
13. Which DOS command is used to copy files? QPO\_\_\_\_\_
14. Which DOS command deletes a file? QPO\_\_\_\_\_
15. Which DOS command renames a file? QPO\_\_\_\_\_
16. Which DOS command will duplicate a disk? QPO\_\_\_\_\_

#### IV. Hard Disk Organization and Maintenance (Mandatory)

##### A. Instruction

1. Watch video entitled "Hard Disk Organization and Maintenance." QPO\_\_\_\_\_

##### B. PQS

1. What function does each of the following routines perform:
  - (a) DOS FDISK QPO\_\_\_\_\_

1 NOV 1994

- (b) DOS CHKDSK QPO\_\_
- (c) PCTOOLS FIXDISK QPO\_\_
- (d) PCTOOLS COMPRESS QPO\_\_

2. Define COMOMAG's disk Backup policy. QPO\_\_

V. Microsoft Word/WordPerfect

A. Instruction

- 1. Watch introductory video for the application. QPO\_\_
- 2. For WordPerfect, complete tasks: QPO\_\_
  - (a) On the introductory diskette. QPO\_\_
  - (b) Outlined in the WordPerfect workbook and hand out. QPO\_\_
- 3. For Microsoft Word, complete the tutorial under the applications HELP menu. QPO\_\_

B. PQS

- 1. Demonstrate the procedures for:
  - (a) Setting tabs and margins. QPO\_\_
  - (b) Setting initial fonts. QPO\_\_
  - (c) Selecting a printer. QPO\_\_
  - (d) Setting a default data directory. QPO\_\_
  - (e) Retrieving a document:
    - (1) From the default directory. QPO\_\_
    - (2) From drive A. QPO\_\_
    - (3) From a different directory. QPO\_\_
  - (f) Storing a document:
    - (1) To default directory. QPO\_\_
    - (2) To drive A. QPO\_\_

1 NOV 1994

- (3) To a different directory. QPO\_\_\_\_\_
- (g) Printing a document. QPO\_\_\_\_\_
2. Demonstrate the following TEXT Editing procedures.
- (a) Cursor movement. QPO\_\_\_\_\_
- (b) Correct a word. QPO\_\_\_\_\_
- (c) Delete a word and sentence. QPO\_\_\_\_\_
- (d) Move a sentence and paragraph. QPO\_\_\_\_\_
3. Demonstrate how to use:
- (a) Spell check. QPO\_\_\_\_\_
- (b) Thesaurus. QPO\_\_\_\_\_
4. Demonstrate the procedures for:
- (a) Importing text. QPO\_\_\_\_\_
- (b) Exporting text. QPO\_\_\_\_\_
- (c) Advanced WP
5. Demonstrate the procedure for:
- (a) Merging documents. QPO\_\_\_\_\_
- (b) Changing Fonts. QPO\_\_\_\_\_
- (c) Importing Graphics. QPO\_\_\_\_\_

## VI. Harvard Graphics

### A. Instruction

1. Complete the tutorial in the Harvard Graphics Users Manual (Chapters 1-4). QPO\_\_\_\_\_

### B. PQS

1. Set the default data directory. QPO\_\_\_\_\_
2. Create a chart. QPO\_\_\_\_\_
3. Retrieve an existing chart. QPO\_\_\_\_\_

1 NOV 1994

4. Demonstrate how to enter text on a chart. QPO\_\_
5. Demonstrate how to retrieve and place symbols or graphic images on a chart. QPO\_\_
6. Save a chart. QPO\_\_
7. Create a presentation. QPO\_\_
8. Add slides to a presentation. QPO\_\_
9. Demonstrate how to select a printer. QPO\_\_
10. Output a chart to a designated printer. QPO\_\_

## VII. PROCOMM Plus

## A. Instruction

1. Complete the tutorial in the ProComm Plus Users Manual (Chapters 1-5) QPO\_\_

## B. PQS

1. Start the program. QPO\_\_
2. Use the Setup Menu to configure the program by:
  - (a) Selecting the communications port. QPO\_\_
  - (b) Setting the baud rate. QPO\_\_
  - (c) Setting the parity. QPO\_\_
  - (d) Changing the data bits setting. QPO\_\_
  - (e) Changing the stop bit setting. QPO\_\_
  - (f) Setting the default directory. QPO\_\_
3. Enter the DIAL SCREEN and dial a number:
  - (a) Manually. QPO\_\_
  - (b) From a dialing entry. QPO\_\_
4. Call the COMOMAG Bulletin Board and:

**1 NOV 1994**

(a) Upload a file.

QPO\_\_\_\_\_

(b) Download a file.

QPO\_\_\_\_\_

## VIII. PKZIP

## A. Instruction

1. Complete the tutorial in the PKZIP Users Manual.

QPO\_\_\_\_\_

## B. PQS

1. Start the program.
2. Zip a File/Directory.
3. Unzip a File/Directory.

QPO\_\_\_\_\_

QPO\_\_\_\_\_

QPO\_\_\_\_\_

## IX. PFS First Choice

## A. Instruction

1. Complete the tutorial in the First Choice Users Manual (Chapters 1 & 2).

QPO\_\_\_\_\_

## B. PQS

1. Configure the program by:

- (a) Setting the default data directory.

QPO\_\_\_\_\_

- (b) Selecting a printer.

QPO\_\_\_\_\_

2. Create and modify a:

- (a) Document.

QPO\_\_\_\_\_

- (b) Database.

QPO\_\_\_\_\_

- (c) Spreadsheet.

QPO\_\_\_\_\_

3. Print a document, database or spreadsheet.

QPO\_\_\_\_\_

4. Retrieve a document, database or spreadsheet.

QPO\_\_\_\_\_

5. Save a document, database or spreadsheet.

QPO\_\_\_\_\_